Department of Veterans Affairs
Washington, DC 20420

VA HANDBOOK 0327
Transmittal Sheet
April 10, 2017

INSIDER THREAT PROGRAM

1. REASON FOR ISSUE: This Insider Threat Program Handbook implements the Insider Threat Program (ITP) within the Department of Veterans Affairs (VA) as prescribed by the VA Directive 0327 (Insider Threat), dated September 2, 2014. This handbook prescribes responsibilities, development, coordination, and implementation of the ITP, as directed by Executive Order (E.O) 13587, "Structural Reforms to Improve the Security of classified Networks and the Responsible Sharing and Safeguarding of Classified Information," issued October 7, 2011 and the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.

2. SUMMARY OF CONTENT/MAJOR CHANGES: This handbook applies to all VA cleared employees as defined in Appendix B. As used in this handbook, the term "cleared employees" does not include any individual who does not have a security clearance. This handbook is effective immediately and applies to all VA administrations and staff offices.

3. RESPONSIBLE OFFICE: The Office of Operations, Security, and Preparedness (007).

4. RELATED DIRECTIVE: VA Directive 0327, Insider Threat Program

5. RECESSION: None

CERTIFIED BY:

/s/
Dat Tran
Acting Assistant Secretary
Office of Enterprise Integration

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS

/s/
Kevin T. Hanretta
Assistant Secretary for
Operations, Security, and Preparedness

This page left intentionally blank.

INSIDER THREAT PROGRAM

Contents

This page left intentionally blank.

1. GENERAL INFORMATION

a. **Purpose**

This Insider Threat Program Handbook implements the Insider Threat Program (ITP) within the Department of Veterans Affairs (VA) as prescribed by the VA Directive 0327 (Insider Threat), dated September 2, 2014. This handbook prescribes responsibilities, development, coordination and implementation of the ITP, as directed by Executive Order (E.O.) 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," Issued October 7, 2011 and the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.

b. **Authority**

The authorities for this guidance are derived from E.O. 13587; E.O. 10450; E.O. 13526; E.O. 12968; the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs; and the VA Directive 0327 (Insider Threat), dated September 2, 2014.

c. **Scope**

This manual applies to all VA **cleared** employees as defined in Appendix B. As used in this Handbook, the term "cleared employees" does not include any individual who does not have a security clearance. This Handbook is effective immediately and applies to all VA administrations and staff offices.

2. RESPONSIBILITIES

a. The National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs directed VA to establish an Insider Threat Program (ITP) to deter cleared employees from becoming insider threats; detect insiders who pose a risk to classified information, wittingly or otherwise; and mitigate the risks through administrative, investigative, and other responses.

(1) In accordance with the published VA ITP Directive, the Assistant Secretary for Operations, Security, and Preparedness (AS for OSP), Senior Agency Official (SAO), has delegated the Deputy Assistant Secretary (DAS) for Emergency Management and Resilience as VA's Senior Insider Threat Official, with the responsibility and authority for the direction, management and implementation of the ITP.

(2) The Senior Insider Threat Official or his/her designees will coordinate with the Office of General Counsel (OGC), Office of Human Resources and Administration (HR&A), Office of Information &Technology (OI&T), Office of the Inspector General (OIG), Office of Privacy and Records Management, and other Administrations and Staff Offices as

applicable and relevant, in the coordination of activities in support of the program. The senior insider threat official will also:

(a) Provide management, accountability, and oversight of the ITP, and make resource recommendations to the VA Secretary via the AS for OSP.

(b) Implement a comprehensive VA Insider Threat Policy.

(c) Ensure the ITP is executed in accordance with all applicable laws and policies.

(d) Establish guidelines and procedures for the retention, sharing, and safeguarding of records and documents necessary to complete insider threat related inquiries and assessments.

(e) Establish oversight mechanisms for proper handling and retention of Insider Threat records restricting them to Insider Threat personnel.

(f) Establish and lead an ITP Executive Steering Committee for consultation on all ITP-related issues, conducting program oversight and reviews, as well as identifying and making program resource recommendations.

(g) Establish an ITP management office with a centralized analysis and response capability to gather, integrate, review, assess, and respond to information derived from counterintelligence, information assurance, security, HR&A, and other information sources as deemed appropriate.

(h) Oversee the collection, analysis, and reporting of information across VA to support the identification and assessment of insider threats.

(i) Establish and manage reporting requirements, to include self-assessments and independent assessments, and reports all findings to the National Senior Information Sharing and Safeguarding Steering Committee.

(j) Establish and execute an Insider Threat Awareness Training Program.

(k) Detail or assign staff, as appropriate and necessary, to the Classified Information Sharing and Safeguarding Office (CISSO) and/or the Insider Threat Task Force (ITTF).

(l) Update this handbook as appropriate.

(3) The Director, Operations and National Security Services (ONSS) will have specific responsibility and authority to administer and coordinate VA’s ITP and will:

(a) Establish and operate VA centralized insider threat analytic and response capability.

(b) Establish and maintain an Insider Threat Awareness Training program for VA employees, and ensure that ITP personnel are fully trained in the subjects required by the Minimum Standards for Executive Branch Insider Threat Programs.

(c) Provide an implementation plan and periodic updates to the DAS, and annually report to the Secretary on the program's progress and status via the AS for OSP.

(d) Provide annual reports to the Senior Information Sharing and Safeguarding Steering Committee, as appropriate.

(e) Facilitate independent assessments by the Executive Agent for Safeguarding Classified Information and the Insider Threat Task Force in accordance with Section 2.1 (d) of E.O. 13587.

(f) Disseminate and implement guidance and procedures related to insider threat reporting, documentation, and actions.

3. INFORMATION INTEGRATION, ANALYSIS, AND RESPONSE

a. **General**

The Director of ONSS and/or the Insider Threat Program Manager (ITPM) will ensure timely access, through electronic means to gather, integrate, centralize, review, assess, and respond to information derived from OGC, HR&A, OI&T, law enforcement, the OIG, or other relevant components.

b. **Information Integration and Analysis**

The ITPM, in collaboration with program components, will establish procedures to collect data and information to identify anomalous behavior that may reveal insider threat activity, such as, information collected from audit data; foreign travel and foreign contact data; financial disclosure data; personnel security vetting data, and human resources, as applicable.

c. **Inquiry/investigative and response actions**

(1) When a potential insider threat is reported or anomalous behavior is detected, the ITPM will direct immediate response action(s) to clarify or resolve the potential insider threat matter. These actions include but are not limited to:

(a) Within forty-eight hours or two business days, determine if collected data or reported behavior/anomaly warrants an insider threat inquiry (an internal inquiry to determine if the threat warrants referral to external investigative entities such as the Federal Bureau of Investigation (FBI), or the Department of Justice), or should the matter be referred to another office/entity, such as OIG, HR&A, Personnel Security, or OI&T, for resolution.

(b) During instances involving national security or matters reasonably likely to result in potential legal action or prosecution, the ITPM will consult with the OGC, advise the OIG, and ensure notification to the FBI and Department of Justice, as required under Section 811 of the Intelligence Authorization Act of Fiscal Year 1995.

(2) If the ITPM determines the need for an insider threat inquiry, the following actions should occur (not necessarily in the order listed), but are not limited to:

(a) Identify an inquiry officer.

(b) Coordinate with VA components for records, analysis, etc., as outlined in Section B of this handbook.

(c) Seek access to the behavioral science services of a psychologist either on staff, under contract, or through an agreement with another Federal agency. This individual should have experience in counterintelligence, security, or insider threat discipline and be able to provide consultation, research, and/or training. This activity will be conducted subsequent to consultation with the OGC.

(d) Conduct interviews.

(e) The investigative period to resolve insider threat inquires shall not exceed ninety days without specific consent from the ONSS Director.

d. **How to handle/report adverse information:**

The ONSS Director and/or the ITPM will report adverse information to the appropriate VA supervisory official and or the Employee Relations office, as appropriate, within 7 days after the conclusion of the insider threat inquiry. An interim report may be provided upon request at the discretion of the reporting official. The ONSS Director shall vary these reporting requirements when, in his or her professional judgment, a faster response is necessary to address a risk of immediate harm.

4. REPORTS

The inquiry officer will complete a written report, documenting response actions performed by insider threat analytic and response capability personnel, with the responsibility for the inquiry. The final report will be submitted to the ONSS Director for final approval.

5. PROPER HANDLING/RETENTION OF RECORDS

a. All records, reports and documentation pertaining to Insider Threat cases will be handled only by Insider Threat personnel or as approved by the ONSS Director and controlled in accordance with guidance from E.O 13526, Classified National Security Information.

b. All VA's Insider Threat records, reports and documentation will be retained indefinitely based on the level of classification outlined in E.O.13526 and handled by only Insider Threat personnel. VA Insider Threat Program will reevaluate this requirement when the National Archives and Records Administration provide General Records Retention Schedule covering the National Insider Threat Program.

6. INSIDER THREAT PROGRAM PERSONNEL

a. **Purpose**

This subpart sets standards for establishing and maintaining tailored training for insider threat analytic and response personnel and other employees depending on mission, access, and vulnerabilities. Such employees include Insider Threat Working Group (ITWG) members, supervisors and managers, information assurance personnel, IT systems administrators and engineers, IT close support team members, investigators, personnel security/suitability adjudicators.

b. **Responsibilities**

(1) The ITWG, chaired by the ONSS Director or designee, consists of representation from VA organizational components, including, but not limited to OGC, HR&A, OIG, and OI&T. The ITWG shall develop and recommend policies and procedures that govern access to, sharing of, and reporting requirements for information necessary to identify, analyze, and resolve insider threat matters pursuant to the tenets of E.O. 13587.

(2) The ONSS Director, in conjunction with the Senior Insider Threat Official, and in conjunction with VA program offices, will designate department personnel to the ITP HUB and ensure the personnel are appropriately trained in counterintelligence, security fundamentals and VA guidelines and procedures for conducting insider threat inquiries and response actions. The ITPM will assist in providing designated HUB members this specific training as available:

(a) Applicable laws and regulations governing privacy and civil liberties.

(b) Safeguarding of records and data, including consequences for misuse of such information.

(c) The investigative referral requirements of Section 811 of the Intelligence Authorization Act of Fiscal Year 1995, as well as other policy or statutory requirements that require referral to internal entities, such as Personnel Security, the OIG, or external investigative entities such as the FBI or the Department of Justice. The Department of Justice is the deciding entity for the U.S. Government in determining a criminal investigating agency, type of criminal investigation and venue for prosecution.

(d) To help determine travel risk, the Director ONSS or ITP personnel should use available classified and unclassified resources, including the following lists:

1. Office of the National Counterintelligence Executive, National Threat Identification and Prioritization Assessment

2. Department of State, Security Environment Threat List

3. Department of State, Travel Warning List

7. ACCESS TO INFORMATION

a. **Purpose**

This subpart sets standards for establishing policies and procedures governing the access to and sharing of pertinent information regarding counterintelligence, security, information assurance, law enforcement, and HR data in the furtherance of the ITP development, implementation, management, and oversight.

b. **Responsibilities**

(1) In coordination with the ITWG, VA organizational components and entities, including but not limited to HR&A, OI&T, OIG, OGC and OSP, shall share data in a timely manner with the insider threat analytic and response personnel. Where possible, they shall provide electronic access to the information necessary to identify, analyze and resolve insider threat matters in accordance with the established reporting guidelines. Such information includes but is not limited to:

(a) Counterintelligence/Security: All information and data derived from relevant databases and files including but not limited to personnel security files, law enforcement files, access records, security violation files, foreign travel records, foreign contact reports, financial disclosure filings, and polygraph examination reports, if applicable.

(b) Information Assurance: All information and data derived from relevant classified and unclassified network information identified as critical IT infrastructure, generated on the OI&T networks including but not limited to personnel usernames and aliases, levels of network access, enterprise audits, unauthorized use of removable media, print logs, and other data needed for clarification or resolution of an insider threat concern.

(c) Human Resources: All information and data derived from relevant HR databases and files including but not limited to personnel files, outside work/activities requests, disciplinary files, and personal conduct records as may be necessary for resolving or clarifying insider threat matters. Requests for payroll and voucher files would be handled through the Office of the Chief Financial Officer. Individual requests for employee information must be reviewed by the appropriate system of records owner to determine what is releasable in accordance with 5 CFR 293.

(2) The ONSS Director or ITPM will provide written or oral justification as it pertains to request involving access to particularly sensitive or protected information, such as information held by OIG, Special Security Office or other investigative sources.

(3) The ITPM will work with component organizations to ensure service level agreements allowing timely access to all relevant classified network information as outlined in paragraphs 1-3 above.

8. MONITORING USER ACTIVITY ON NETWORKS

a. **General**

User activity is monitored on VA IT automated systems, infrastructure, and networks. This monitoring includes but is not limited to:

(1) Logons/logoffs

(2) File and object access

(3) User and group management

(4) Security and audit policy changes

(5) System starts/shutdowns

(6) File and object manipulation, such as addition, deletion, and modification, including change of permissions and/or ownership

(7) Print activity

(8) Use of privileged/special rights

(9) Writes/downloads to local devices, such as USB drives, DVDs, and CD-ROMs

(10) Uploads from local devices

(11) File(s) printed to include descriptive information, enabling identification of printed item

(12) Root-level access

(13) Query strings

(14) Query results

b. **Responsibilities**

(1) The ITPM shall collaborate with VA OI&T and OGC concerning user monitoring for all VA employees with access to the unclassified network. ITPM shall also coordinate with classified network service providers to ensure service level agreements contain language for them to monitor user activity on all cleared VA employees on their systems. This will be done in order to detect activity indicative of insider threat behavior, outline the capabilities the provider will employ to identify suspicious user behavior, and indicate how that information shall be reported to the insider threat personnel. VA ITPM will reevaluate all service level agreements annually during the self-assessment process.

(2) OI&T establishes, maintains and monitors Department-wide information security policies, procedures, control techniques, training, and inspection requirements as elements of the VA information security program. This is done while maintaining the technical capability to monitor user activity on VA unclassified networks as outlined in the VA Handbook 6500.3.

(3) The Chief Information Officer (CIO) will establish and implement policies and procedures on VA unclassified networks for properly protecting, interpreting, storing, and limiting access to user activity monitoring methods and results to authorized personnel within the ITP.

(4) The OSP will establish and implement policies and procedures for VA cleared employees to sign agreements acknowledging that their activity on any classified network, is subject to monitoring and could be used against them in a criminal, security, or administrative proceeding.

(5) The OI&T and OSP will ensure network banners on unclassified and classified networks inform users that their activity on the network is being monitored for lawful U.S. Government-authorized purposes and can result in criminal or administrative actions against the user.

9. EMPLOYEE TRAINING AND AWARENESS

a. **Purpose**

This section sets standards for VA's Insider Threat Awareness Training Program. The Insider Threat Awareness Training Program shall ensure all VA cleared employees are aware of VA policies and guidelines. VA cleared employees will receive comprehensive training as part of VA's Safeguarding National Security Information Training, required under EO 13526. VA employees will also receive supplemental training on Insider Threat Awareness topics and other sessions, as necessary. The Insider Threat Awareness Training will address current and potential threats in the work and personal environment and shall include, at a minimum, the following topics:

(1) The importance of detecting potential insider threats

(2) The importance of reporting suspicious activity to ITP response personnel

(3) Methodologies of adversaries to recruit trusted insiders and collect classified information

(4) Indicators of insider threat behavior and procedures to securely report such behavior, and

(5) Counterintelligence and security reporting requirements

b. **Responsibilities**

The Director, ONSS is responsible for the Insider Threat Awareness Training Program, and shall determine the means, methods, and intervals for providing Insider Threat Awareness Training. The Insider Threat Awareness Program will be tailored to meet the specific needs and responsibilities of the cleared employees. The frequency of VA Insider Threat Awareness Training will vary in accordance with the needs of the Agency's ITP, subject to the following requirements:

c. **Approach**

The Senior Insider Threat Official or his/her designee will leverage relevant VA components and their Federal partners to meet ITP training initiatives. Training methods may include in-person briefings, interactive videos, dissemination of instructional materials, online presentations, media, and other methods. Records about the programs that were offered and employee participation shall be maintained and subject to the following requirements:

(1) Initial Insider Threat Awareness Training will be provided to VA cleared employees.

(2) Annually, VA cleared employees will be provided Insider Threat Awareness Training to remind them of awareness and reporting requirements.

(3) To achieve desired results, all training should be conducted initially in person to the maximum extent possible.

(4) The training may be provided through the web-based Talent Management System (TMS).

(5) The Senior Insider Threat Official or his/her designee may grant a waiver of this requirement if an individual is unable to receive this training due to unavoidable circumstances. All such waivers shall be documented.

10. REPORTING REQUIREMENTS FOR VA EMPLOYEES

a. **Purpose**

This subpart sets standards for establishing reporting requirements for VA employees to the ITP. As directed by Presidential Decision Directive (PDD/NSC-12), "Security Awareness and Reporting of Foreign Contacts" and other federal and agency policies, VA cleared employees are required to report to VA ITP or SSO all contacts with individuals of any nationality, either within or outside the scope of the employee's official activities, whenever:

(1) An individual or group seeks illegal or unauthorized access to classified or otherwise sensitive information, or

(2) The employee is concerned that he/she may be the target of actual or attempted exploitation by a foreign entity.

b. **Responsibilities**

(1) The Director, ONSS shall establish procedures and a secure method for cleared employees to report insider threat-related incidents, behavioral indicators or other matters to ITP personnel. Established reporting procedures must ensure that employees feel confident they can make a report without fear of reprisal.

(2) VA cleared employees must report behavioral threat indicators or incidents to VA Security (see Appendix C). All reported information, including the identity of the person making the report, will be treated with strict confidentiality.

(3) VA employees and/or supervisors must not obstruct or impede any cleared employee from reporting insider threat related incidents, behavioral indicators, or other matters to VA ITP personnel.

(4) Personnel who report insider threat-related incidents, behavioral indicators or other matters that are intentionally false or fabricated may be subject to disciplinary, administrative, and/or legal action.

11. REPORTING

Annual Reporting Requirements

(a) Progress and Status Statistical Reporting: The Department's Senior Insider Threat Official shall report annually to the Office of the Secretary on the progress and/or status of the ITP via AS for OSP. At a minimum, the annual report shall document annual accomplishments, resources allocated, insider threat risks to the agency, recommendations and goals for program improvement, and major impediments or challenges. He/She will provide instructions to organizations regarding what data elements

are required, and how and when they are to be reported. He/She will also report the findings to the Senior Information Sharing and Safeguarding Steering Committee.

(b) Self-Inspections: The ITPM will ensure self-inspections of the program are performed annually. The ITPM will also facilitate as needed oversight reviews by the Office of the Inspector General or any cleared officials designated by the Secretary for compliance with insider threat policy guidelines, as well as applicable legal, privacy, and civil liberty protections.

(c) Investigative Referral/Reporting Requirements

(1) Insider threat response action(s) that involve administrative, security, or law enforcement implications shall be reported to the appropriate internal VA organization, i.e., Employee Relations, VA Police, or OIG.

(2) Insider threat response action(s) that could involve espionage shall be promptly reported to OGC and the FBI, in compliance with the Privacy Act and other applicable laws.

APPENDIX A

1. **References**

a. Executive Order 13587 of October 7, 2011, “Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information”

b. White House Memorandum of November 21, 2012, “National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs”

c. Executive Order 13526 of December 29, 2009, “Classified National Security Information”

d. Executive Order 12968 of August 4, 1995, “Access to Classified Information”

e. 32 C.F.R. Part 2001, “Classified National Security Information”

f. White House Memorandum of August 23, 1996, “Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies”

g. Section 811 of the Intelligence Authorization Act for Fiscal Year 1995

h. Presidential Decision Directive/NSC-12 of August 5, 1993, “Security Awareness and Reporting of Foreign Contacts Security Awareness and Reporting of Foreign Contacts, Presidential Decision Directive” (PDD/NSC-12, 05 August 1993)

i. Executive Order 12333 of December 4, 1981 (Amended), “United States Intelligence Activities”

j. Executive Order 10450 of April 27, 1953, “Security Requirements for Government Employment”

k. VA Insider Threat Directive 0327, dated September 2, 2014

APPENDIX B

1. DEFINITIONS

a. Agency: Any “Executive agency,” as defined in 5 U.S.C. 105, and the U.S. Postal Service; any “Military Department” as defined in 5 U.S.C. 102; and any other entity within the executive branch that uses, handles, or stores unclassified and/or classified information or has positions as sensitive, except such an entity headed by an officer who is not a covered individual.

b. Anomaly: Activity or knowledge, outside the norm, that suggests a foreign entity has foreknowledge of U.S. information, processes, or capabilities.

c. Classified information: Information that has been determined pursuant to EO 13526 or any successor order, EO 12951 or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure and that it is marked to indicate its classified status when in documentary form.

d. Cleared Employee: A VA employee as defined in this appendix, who has been granted eligibility for access to classified information at the Confidential, Secret, or Top Secret level, and who has signed an approved nondisclosure agreement (Standard Form 312), regardless of whether his/her eligibility for access is active or suspended.

e. Counterintelligence: Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons or their agents, or international terrorist organizations or activities.

f. Employee: An “employee” as defined in section 1.1(e) of EO 12968, as amended, including an VA employee; or a contract employee, detailee/assignee, expert, consultant, licensee, grantee, or certificate holder who acts for or on behalf of VA.

g. Foreign National: Any person who is not a citizen or national of the United States.

h. Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, which is owned by, is produced by or for, or is under the control of the U.S. Government.

i. Insider: Any person with authorized access to any U.S. Government (USG) resource, including personnel, facilities, information, equipment, networks, or systems.

j. Insider Threat: The threat that an insider will use his/her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the U.S. through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of agency resources or capabilities.

k. Insider Threat Response Action(s): Activities to ascertain whether certain matters or information indicates the presence of an insider threat, as well activities to mitigate the threat. Such an inquiry or investigation can be conducted under the auspices of counterintelligence, security, law enforcement, or inspector general elements, depending on statutory authority and internal policies governing the conduct of such activity in each agency.

l. Safeguarding: Measures and controls that are prescribed to protect classified information from unauthorized access and to manage the risks associated with processing, storage, handling, transmission, and destruction of classified information.

m. Unauthorized Disclosure: A communication, confirmation, acknowledgement, or physical transfer of classified including the facilitation of, or actual giving, passing, selling, publishing, or in any way making such information available to an unauthorized recipient.

APPENDIX C

1. LIST OF REPORTABLE ACTIVITIES

a. VA employees are required to report to ITP personnel information regarding other VA employees that exhibit any of the behaviors listed in tables 1, 2, and 3 below. A single behavioral indicator by itself does not necessarily mean that a person is involved in activities that threaten VA or the U.S. However, reporting the behavior to the ITP personnel will allow them to appropriately assess the threat potential or, if appropriate, refer the incident to another agency. Tables 1 through 3 contain reportable contacts, activities, indicators, behaviors, and cyber threats.

Table 1. Reportable Contacts, Activities, Indicators, and Behaviors

1.	When not related to official duties, contact with anyone known or believed to have information of planned, attempted, actual, or suspected espionage, sabotage, subversion, or other intelligence activities against facilities, organizations, personnel, or information systems. This includes contact through social networking sites that is not related to official duties.
2.	Attempts by anyone, regardless of nationality, to obtain or acquire unauthorized access to classified or sensitive information in the form of facilities, activities, personnel, technology, or material through any of the following methods: questioning, elicitation, trickery, bribery, threats, coercion, blackmail, photography, observation, collection of documents or material, correspondence (including electronic correspondence), or automated systems intrusions.
3.	Contact with an individual who is known or suspected of being associated with a foreign intelligence or security organization.
4.	Visits to foreign diplomatic facilities that are unexplained or inconsistent with an individual's official duties.
5.	Acquiring, or permitting others to acquire, unauthorized access to classified information systems.
6.	Attempts to obtain classified information by an individual not authorized to receive such information.
7.	Persons attempting to obtain access to information inconsistent with their duty requirements.
8.	Attempting to expand access to classified information by volunteering for assignments or duties beyond the normal scope of responsibilities.
9.	Discovery of suspected listening or surveillance devices in classified or secure areas.
10.	Unauthorized possession or operation of cameras, recording devices, computers, and communication devices where classified information is

	handled or stored.
11.	Discussions of classified information over a non-secure communication device.
12.	Reading or discussing classified information in a location where such activity is not permitted.
13.	Transmitting or transporting classified information by unsecured or unauthorized means.
14.	Removing or sending classified material out of secured areas without proper authorization.
15.	Unauthorized storage of classified material, regardless of medium or location, including unauthorized storage of classified material at home.
16.	Unauthorized copying, printing, faxing, e-mailing, or transmitting classified material.
17.	Improperly removing classification markings from documents or improperly changing classification markings on documents.
18.	Suspiciously working outside of normal duty hours.
19.	Attempts to entice co-workers into criminal situations that could lead to blackmail or extortion.
20.	Attempts to entice personnel or contractors into situations that could place them in a compromising position.
21.	Attempts to place personnel or contractors under obligation through special treatment, favors, gifts, or money.
22.	Requests for witness signatures certifying the destruction of classified information when the witness did not observe the destruction.
23.	Requests for information that make an individual suspicious, including suspicious or questionable requests over the internet or social networking sites.
24.	Trips to foreign countries that are: • Short trips inconsistent with logical vacation travel or not part of official duties. • Trips inconsistent with an individual’s financial ability and official duties.
25.	Personnel who are in contact with any official or citizen of a foreign country when the foreign official or citizen: • Exhibits excessive knowledge of or undue interest in personnel or their duties beyond the normal scope of friendly conversation. • Attempts to obtain classified or unclassified information. • Attempts to place personnel under obligation through special treatment, favors, gifts, money, or other means. • Attempts to establish business relationships that are outside the scope of

	normal official duties.
26.	Incidents in which personnel or their family members traveling to or through foreign countries are contacted by persons who represent a foreign law enforcement, security or intelligence organization and • Are questioned about their duties. • Are requested to provide classified or unclassified information. • Are threatened, coerced or pressured in any way to cooperate with the foreign official. • Are offered assistance in gaining access to people or locations not routinely afforded Americans.
27.	Unexplained or undue affluence. • Expensive purchases an individual's income does not logically support. • Attempts to explain wealth by reference to inheritance luck in gambling, or a successful business venture. • Sudden reversal of a bad financial situation or repayment of large debts.
28.	Contacts with individuals of any nationality, either within or outside the scope of the employee's official activities, in which: • Illegal or unauthorized access is sought to classified or otherwise sensitive information. • The employee is concerned that he/she may be the target of actual or attempted exploitation by a foreign entity.
29.	Any contact with the media where the media seeks access to or results in the unauthorized disclosure of classified information.
30.	Specific adverse changes to financial status, i.e., garnishments, foreclosures, liens, judgments, delinquent taxes, and/or bankruptcy filings.
31.	Any hospitalization for a mental health condition.
32.	Use of or involvement with illegal drugs or controlled substances, and/or the misuse of prescription/legal drugs or dangerous inhalants.
33.	Criminal conduct.
34.	Any activity that could constitute a conflict of interest with U.S. Government employment.
35.	Suspected illegal use of U.S. Government property of information systems.

Table 2: Reportable Suspected Terrorism or Work place Violence Contacts, Activities, Indicators, and Behaviors

1.	Advocating violence, the threat of violence, or the use of force to achieve goals on behalf of a known or suspected international terrorist organization.
2.	Advocating support for a known or suspected international terrorist organizations or objectives.
3.	Providing financial or other material support to a known or suspected international terrorist organization or to someone suspected of being an international terrorist.
4.	Procuring supplies and equipment, including purchasing bomb making materials or obtaining information about the construction of explosives, on behalf of a known or suspected international terrorist organization.
5.	Contact, association, or connections to known or suspected international terrorists, including online, e-mail, and social networking contacts.
6.	Expressing an obligation to engage in violence in support of known or suspected international terrorism or inciting others to do the same.
7.	Any attempt to recruit personnel on behalf of a known or suspected international terrorist organization or for terrorist activities.
8.	Collecting intelligence, including information regarding installation security, on behalf of a known or suspected international terrorist organization.
9.	Familial ties, or other close associations, to known or suspected international terrorists or terrorist supporters.
10.	Repeated browsing or visiting known or suspected international terrorist websites that promote or advocate violence directed against the United States or U.S. forces, or that promote international terrorism or terrorist themes, without official approval in the performance of duty.
11.	Possessing weapons in the work place.
12.	Threatening to kill or harm supervisors, co-workers, or anyone else within or outside of the work place.
13.	Sending emails or posting on social media sites threatening communications against supervisors, co-workers, or anyone else within or outside of the work place.

Table 3: Reportable Behaviors Associated With Information Technology Systems and Cyberspace Contacts, Activities, and Indicators

1.	Actual or attempted unauthorized access into U.S. automated information systems and unauthorized transmissions of U.S. Government information.
2.	Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.
3.	Network spillage incidents or information compromise.
4.	Use of account credentials by unauthorized parties.
5.	Tampering with or introducing unauthorized elements into information systems.
6.	Unauthorized downloads or uploads of sensitive data.
7.	Unauthorized use of Universal Serial Bus, removable media, or other transfer devices.
8.	Downloading or installing non-approved computer applications.
9.	Unauthorized network access.
10.	E-mail correspondence with foreign nationals.
11.	Denial of service attacks or suspicious network communications failures.
12.	Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.
13.	Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage.
14.	Data ex-filtrated to unauthorized domains.
15.	Unexplained storage of encrypted data.
16.	Unexplained user accounts.
17.	Hacking or cracking activities.
18.	Social engineering, electronic elicitation, e-mail spoofing or spear phishing.
19.	Malicious codes or blended threats such as viruses, worms, Trojan horses, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration.